“良い” 符号であるためには、

符号語が “均等” に散らばっているのが
望ましかった。

平行移動で重なる $\longrightarrow$ 線型符号

もっと “対称性” が高いと良いのでは ？

“対称性” $\longrightarrow$ 符号の自己同型

符号の自己同型

$\mathcal{C}$: 符号 $\subset V = \boldsymbol{F}_q^n$

f : $\mathcal{C}$ の 自己同型

$\Longleftrightarrow f : V \longrightarrow V$: 等距離線型同型で $f(\mathcal{C}) = \mathcal{C}$

その全体は群を成す $\cdots \mathrm{Aut}(\mathcal{C})$

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V, d) = \mathfrak{S}_n \wr \boldsymbol{F}_q^{\times}$$

符号の自己同型

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n \wr \boldsymbol{F}_q^{\times}$$

特に、$q = 2$ のときは、

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n$$

$\longrightarrow$ **対称群の有限体上の線型表現の問題に**

典型的な場合:

$\sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$ **のとき**

$\cdots$ **巡回符号 (cyclic code)**

巡回符号

$\mathcal{C}$: **巡回符号**

$\Longleftrightarrow \sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$

$\Longleftrightarrow$

「$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Longrightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$」

$$\sigma = (1\ 2\ \cdots\ n) \in \mathfrak{S}_n, \sigma^n = 1$$

$$\boldsymbol{F}_q[\langle\sigma\rangle] \simeq \boldsymbol{F}_q[X]/(X^n - 1) =: R \curvearrowright V = \boldsymbol{F}_q^n$$

により、V：階数 1 の自由 R-加群

$$V = \boldsymbol{F}_q^n \ \simeq \ R$$
$$(1, 0, \ldots, 0) \leftrightsquigarrow 1$$
$$(c_0, c_1, \ldots, c_{n-1}) \leftrightsquigarrow c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

$\mathcal{C}$: **巡回符号** $\Longleftrightarrow$ $\mathcal{C}$: **部分** R-**加群**

$V \simeq R$ **と同一視するとき**

$\Longleftrightarrow$ $\mathcal{C}$: R **の ideal**

R : **可換環 に対し、**

$\mathfrak{a}$: R **の ideal** $\Longleftrightarrow$

- $\forall a, b \in \mathfrak{a} : a + b \in \mathfrak{a}$
- $\forall a \in \mathfrak{a}, \forall r \in R : ra \in \mathfrak{a}$

$\mathcal{C}$: 巡回符号

$\longleftrightarrow$ $R = \boldsymbol{F}_q[X]/(X^n - 1)$ の ideal $\mathfrak{a}$

$\longleftrightarrow$ $\mathfrak{a} \supset (X^n - 1)$ なる $\boldsymbol{F}_q[X]$ の ideal $\mathfrak{a}$

($\boldsymbol{F}_q[X]$: PID なので $\exists f \in R : \mathfrak{a} = (f)$)

$\longleftrightarrow$ $f | X^n - 1$ なる $f \in \boldsymbol{F}_q[X]$

$X^n - 1 \in \boldsymbol{F}_q[X]$ の分解が判れば、
巡回符号が分類・構成できる !!

$X^n - 1 = g(X)h(X) \in \boldsymbol{F}_q[X]$ **のとき、**

$$\mathcal{C} := gR \text{：} \textbf{巡回符号} \ \simeq \boldsymbol{F}_q[X]/(h)$$
$$= \{c(X) \in R | h(X)c(X) = 0 \ \textbf{in} \ R\}$$

g：**生成元多項式 (generator polynomial)**

h：**検査多項式 (check polynomial)**

$X^n - 1 \in \boldsymbol{F}_q[X]$ **の分解はどうなるのか ？**

$\longrightarrow$ **有限体の拡大・Galois 理論**